IDS Meeting Minutes
June 24, 2021

This IDS Meeting was started at approximately 3:00 pm ET on June 24, 2021.

Attendees

Graydon Dodson	Lexmark
Matt Glockner	Lexmark
Erin Huber	Xerox
Alan Sukert	
Bill Wagner	TIC
Brian Volkoff	Ricoh
Steve Young	Canon

Agenda Items

1. The topics to be covered during this meeting were:
   - Review of the discussions at 6/14/21 and 6/22/21 HCD iTC Meetings
   - Special Topic
   - Round Table Discussion
2. Meeting began by stating the PWG Anti-Trust Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-antitrust- policy.pdf and the PWG Intellectual Property Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-ip-policy.pdf.
3. Al reviewed what was discussed at the 6/14/21 and 6/22/21 Hardcopy Device international Technical Community (HCD iTC) Meetings. The main topics discussed at these meeting was:
   - There was a review of the updated JBMIA proposal for the **FPT_KYP_EXT.1 Protection of Key and Key Material** SFR. JBMIA had presented the proposal at a previous meeting to update the Assurance Activities for this SFR, but it was mentioned that NIAP has issued Technical Decision (TD) 0485 against the **FPT_KYP_EXT.1** Assurance Activities. So JBMIA was asked to incorporate the NIAP TD into its proposal. At the 6/22/21 meeting the HCD iTC reviewed and approved the updated proposal incorporating the NIAP TD.
   - The HCD iTC also reviewed several comments against the HCD cPP generated in response to actions taken by the HCD iTC Hardware-anchored Integrity Verification Subgroup. These comments included:
     - Update FPT_SBT_EXT.1.3 (1) add an additional assignment option to the selection and to (2) add the phrase "so that the corrupted software/firmware isn't invoked" to the end of the element were both acceptable, although the subgroup felt that 'executed" was a better term than 'invoked'.
     - Add a definition of 'Root of Trust' to the Glossary
     - Add a "hardware-anchored firmware/software integrity verification" sentence to the Trusted Operation subsection under Major Security Functions of the HCD
   - Al reviewed the status of the HCD iTC schedule:
     - The 3rd internal drafts of the HCD cPP and HCD SD were supposed to be submitted for review on 6/1. However, the HCD cPP 3rd internal draft wasn't available until 6/9 and the 3rd internal HCD SD draft won't be available until 6/28.
     - Based on that we will almost certainly miss the 7/18 scheduled date for submittal of the 1st Public Review draft. Al's guess is that we are about 3 weeks behind schedule.

- In response to a question Al stated that the 1st Public Review draft will not contain full content as planned; there will be some issues that will not be settled by the end of July.
- Al is still hopeful we will be able to make the 11/1 date for submittal of the 2nd Public Review draft which will have to have full content.

- Al then quickly discussed the current status of the HCD iTC's Hardware-anchor Integrity Verification Subgroup:
  - The subgroup at the last two meetings addressed the issue of the 'contact vendor support' option in FPT_SBT_EXT.1.4 and, based on a comment from Ohya-san, came up with a resolution of changing the wording of that option to 'indicate a need to contact vendor support'.
  - Based on another comment from Ohya-san the subgroup looked into including an SFR for CMAC. Ohya-san submitted a proposal and there was also a CMAC SFR that the Full Disk Encryption (FDE) cPPs had included. Ohya-san was going to look at the two and determine which of the two he thought was better.
  - The subgroup determined the list of items that remained to be addressed:
    - Protection of storing Symmetric keys for message authentication
    - Agree on CMAC SFR
    - Review/update the Assurance Activities for the Secure Boot SFR
    - Add app notes to describe expectations for evaluating hardware Root of Trust (RoT)
    - Add wording to the HCD cPP to more clearly describe connection between hardware-anchored and RoT

4. Al then discussed a meeting he attended on 6/21. The CC Development Board (CCDB) has approved changes to the iTC development process that will have some important impacts to future iTCs. The key changes to the process are:
   - A request to initiate an iTC for a particular class of products currently can only come from a member nation of the CCDB. The CCDB has changed that so that anyone can request that an iTC be created for a particular class of products. That means that, for example, a 3D printer vendor could request to the CCDB that an iTC be formed to create a cPP for 3D printers. However, the process still would require that the iTC would have to be sponsored by two member nations of the CCDB and that a Working Group consisting of at least those two sponsor nations would have to be formed to create the Essential Security Requirements Document.
   - The biggest and most impact full change is that all of the steps that included creation and public review of the Security Problem Definition, submittal and review of Position Statements, development of requirements by the iTC, development, public review and comment resolution of the cPP and SD have all be replaced by one single step – Develop the CPP and SD.
   - The final two steps regarding approving the SD will be replaced because what is currently document does not reflect what is actually being done in practice. Typically, what is done is that the SDs get approved via being certified by the evaluation lab the first time the cPP and SD are used to certify a product. The process will be updated to reflect this.

   In response to a question, Al stated that no specific date was given when the changes will become effected. A draft of the updated process is to be made available for review soon, but it will probably be 4-6 months before the update process is published by the CCDB in the Common Criteria portal.

5. Al then presented his special topic. He discussed the new Executive Order on Improving the Nation's Cybersecurity issued by the White House on May 12, 2021. The reason for discussing the Executive Order was that he felt there were provisions in this document that could have significant impact on the software community because its provisions would apply to any contractor that does business with the Federal Government.

Al prepared some slides on this Executive Order which can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/Cybersecurity Executive Order.pdf. A few key takeaways from the slides:

- The two key provisions that Al believes will most impact IDS members are Cyber Incident Reporting and Enhancing Software Supply Chain Security
- What is interesting about Cyber Incident Reporting is that the definition of "incident" that the Executive Order uses is based on the standard security concepts of jeopardizing Confidentiality, Integrity and Availability.
- The key points in the Enhancing Software Supply Chain Security portion of the Executive Order are:
    - NIST is required to develop guidelines on how software suppliers are to handle supply chain security. Once NIST issues these guidelines it will be interesting to see what organizations like NIAP do with these guidelines.
    - The guidelines shall include criteria that can be used to evaluate software security, include criteria to evaluate the security practices of the developers and suppliers themselves, and identify innovative tools or methods to demonstrate conformance with secure practices. Al mentioned that Common Criteria might provide a good mechanism for demonstrating this conformance with software practices.
    - The guidelines will cover important and familiar security-related issues like (1) multi-factor, risk-based authentication and conditional access; (2) employing encryption for data; (3) ensuring the integrity of the code; (4) check for known and potential vulnerabilities and remediate them; (5) providing a purchaser a Software Bill of Materials (SBOM) for each product; (6) participating in a vulnerability disclosure program that includes a reporting and disclosure process; (7) attesting to conformity with secure software development practices and (8) ensuring integrity and provenance of open source software used within any portion of a product.

There main takeaway is that "the devil will be in the details" in terms of how this Executive Order gets implemented over the next several months.

6. Ira was not present so there was no HCD Security Guidelines status update.
7. There was no Round Table discussion.
8. **Actions:** None

Next Steps

- The next IDS Meeting will be July 8, 2021 at 3:00P ET / 12:00N PT. Main topics will be review of the 6/14/21 & 6/21/21 HCD iTC Meetings, Paul Tykodi's monthly 3D Printing report and HCD Security Guidelines Status Update.